

**PIERCE BAINBRIDGE BECK PRICE
& HECHT LLP**

Thomas D. Warren (SBN No. 160921)
twarren@piercebainbridge.com
Andrew Calderón (SBN No. 316673)
acalderon@piercebainbridge.com
355 S. Grand Avenue, 44th Floor
Los Angeles, CA 90071
Telephone: (213) 262-9333
Facsimile: (213) 279-2008

Dwayne D. Sam (*admitted pro hac vice*)
dsam@piercebainbridge.com
600 Pennsylvania Avenue NW
South Tower, Suite 700
Washington, DC 20004
Telephone: (202) 843-8342
Facsimile: (646) 968-4125

Counsel for Plaintiff Robert Ross

UNITED STATES DISTRICT COURT
NORTHER DISTRICT OF CALIFORNIA
OAKLAND DIVISION

ROBERT ROSS,
Plaintiff,
v.
AT&T MOBILITY, LLC,
Defendant.

Case No. 4:19-CV-06669 (JST)

**PLAINTIFF ROBERT ROSS'S
OPPOSITION TO DEFENDANT AT&T
MOBILITY LLC'S MOTION TO DISMISS
THE COMPLAINT**

Action Filed: October 17, 2019

Hearing:

Date: February 12, 2020

Time: 2:00 p.m.

Place: 1301 Clay Street, 2nd Floor

Courtroom 6

Oakland, CA 94612

Judge: Hon. Jon. S. Tigar

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	ARGUMENT	2
A.	Standard of Review	2
B.	Mr. Ross Adequately Alleged Proximate Cause.....	2
1.	Mr. Ross Adequately Alleged How AT&T’s Swapping of His SIM Card to a Different Phone Led to the Loss of \$1 Million.	2
2.	Mr. Ross’ Allegations Do Not Rely on Unforeseeable Criminal Acts.	5
C.	Mr. Ross’ Right to Privacy Claim Under the California Constitution (Count III) Should Not Be Dismissed Because He Adequately Pled that Actions By AT&T’s Employees Constitute an Egregious Breach of Social Norms.	8
D.	Mr. Ross Specifically Alleged What Information AT&T Disclosed.....	9
E.	Mr. Ross’ Claims for Negligence and Negligent Supervision and Entrustment (Counts IV and V) Should Not Be Dismissed, Given the Existence of a Special Relationship.....	10
F.	Under the CLRA, Mr. Ross Adequately Pled Actual Reliance Based on His Reliance On AT&T’s Privacy Policy.	15
G.	Mr. Ross Adequately Pled Qualifying Loss Under the CFAA.....	16
H.	Punitive Damages Should Not be Stricken.....	17
III.	CONCLUSION.....	19

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	2, 19
<i>Bell Atl. v. Twombly</i> , 550 U.S. 544 (2007).....	1, 2, 5
<i>Bigbee v. Pac. Tel. & Tel. Co.</i> , 34 Cal. 3d 49 (1983)	6
<i>Cabral v. Supple, LLC</i> , 2012 WL 12895825 (C.D. Cal. Oct. 3, 2012).....	10
<i>Campodonico v. State Auto Parks, Inc.</i> , 10 Cal. App. 3d 803 (1970)	6
<i>Castillo v. Seagate Tech., LLC</i> , 2016 WL 9280242 (N.D. Cal. Sept. 14, 2016)	13
<i>Chanda v. Fed. Home Loans Corp.</i> , 215 Cal. App. 4th 746 (2013)	6
<i>City & Cnty. of San Francisco v. Cambridge Integrated Servs. Grp, Inc.</i> , 2007 WL 1970092 (N.D. Cal. July 2, 2007).....	11
<i>CoreLogic, Inc. v. Zurich Am. Ins. Co.</i> , 2016 WL 4698902 (N.D. Cal. Sept. 8, 2016)	11
<i>Corona v. Sony Pictures Entm't, Inc.</i> , 2015 WL 3916744 (C.D. Cal. May 9, 2015)	13
<i>Cytokinetics, Inc. v. Pharm-Olam Int'l, Ltd.</i> , 2015 WL 1056324 (N.D. Cal. Mar. 10, 2015).....	11
<i>DeSoto v. Yellow Freight Sys., Inc.</i> , 957 F.2d 655 (9th Cir. 1992)	2
<i>Doe I v. AOL LLC</i> , 719 F. Supp. 2d 1102 (N.D. Cal. 2010)	15
<i>Dubbs v. Glenmark Generics Ltd.</i> , 2014 WL 1878906 (C.D. Cal. May 9, 2014)	13
<i>Exxon Mobil Oil Corp. v. S. Cal. Edison Co.</i> , 2013 WL 12166214 (C.D. Cal. May 1, 2013)	19

1	<i>In re Facebook, Inc. Sec. Litig.</i> ,	
	405 F.Supp.3d 809 (N.D. Cal. 2019)	15
2	<i>Fields v. Wise Media, LLC</i> ,	
3	2013 WL 5340490 (N.D. Cal. Sept. 24, 2013)	12
4	<i>Flores v. Adir Int'l, LLC</i> ,	
5	685 F. App'x 533 (9th Cir. 2017)	2
6	<i>Henson v. Turn, Inc.</i> ,	
	2018 WL 6605624 (N.D. Cal. 2018)	10
7	<i>Herrera v. Cnty. of Los Angeles</i> ,	
8	2013 WL 12121879 (C.D. Cal. Aug. 2, 2013).....	3, 5
9	<i>In re iPhone Litigation</i> ,	
10	844 F. Supp. 2d 1040 (N.D. Cal. 2012)	9
11	<i>Isaacs v. Huntington Mem'l Hosp.</i> ,	
	38 Cal. 3d 112 (1985)	6
12	<i>J'Aire Corp. v. Gregory</i> ,	
13	24 Cal. 3d 799 (1979)	12, 13, 14, 15
14	<i>Jesse v. Malcmacher</i> ,	
15	2016 WL 9450683 (C.D. Cal. Apr. 5, 2016)	7
16	<i>Khan v. 7-Eleven, Inc.</i> ,	
	2015 WL 12743691 (C.D. Cal. Nov. 15, 2015).....	19
17	<i>Ladore v. Sony Computer Entm't Am., LLC</i> ,	
18	75 F. Supp. 3d 1065 (N.D. Cal. 2014)	11
19	<i>In re: Lenovo Adware Litig.</i> ,	
20	2016 WL 6277245 (N.D. Cal. Oct. 27, 2016).....	17
21	<i>Lies v. Farrell Lines, Inc.</i> ,	
	641 F.2d 765 (9th Cir. 1981)	3
22	<i>Mangiaracina v. Penzone</i> ,	
23	849 F.3d 1191 (9th Cir. 2017)	2
24	<i>Martinez v. Pac. Bell</i> ,	
25	225 Cal. App. 3d 1557 (2003)	5
26	<i>Mass Mut. Life Ins. Co. v. Sup. Ct.</i> ,	
	119 Cal. Rptr. 2d 190, 97 Cal. App. 4th 1282 (Cal. App. 4 Dist. 2002).....	15
27	<i>Moreno v. Sanchez</i> ,	
28	106 Cal. App. 4th 1415 (2003)	11

1	<i>N. Am. Chem. Co. v. Sup. Ct.</i> ,	
2	59 Cal. App. 4th 764 (1997)	11
3	<i>N. Am. Chem. Co. v. Sup. Ct.</i> ,	
4	69 Cal. Rptr. 2d 466 (Cal. App. 2 Dist. 1997)	14
5	<i>NovelPoster v. Javitch Canfield Grp.</i> ,	
6	140 F. Supp. 3d 954 (N.D. Cal. 2014)	17
7	<i>O’Keeffe v. Inca Floats, Inc.</i> ,	
8	1997 WL 703784 (N.D. Cal. Oct. 31, 1997).....	7
9	<i>Ott v. Alfa-Laval Agri, Inc.</i> ,	
10	37 Cal.Rptr.2d 790, 31 Cal.App.4th 1439 (Cal.App. 5 Dist. 1995).....	12
11	<i>Paterson v. Cal. Dept. of Gen. Servs.</i> ,	
12	2008 WL 4737118 (E.D. Cal. Oct. 28, 2008)	18
13	<i>People v. Schmies</i> ,	
14	44 Cal. App. 4th 38 (1996)	7
15	<i>quoting Simplicity Int’l v. Genlabs Corp.</i> ,	
16	2010 WL 11515296 (C.D. Cal. Apr. 21, 2010)	19
17	<i>Ray v. BlueHippo Funding, LLC</i> ,	
18	2008 WL 1995113 (N.D. Cal. May 6, 2008)	12
19	<i>Rios v. City of Bakersfield</i> ,	
20	2011 WL 5554506 (E.D. Cal. Nov. 15, 2011).....	18
21	<i>Rosh v. Cave Imaging Sys., Inc.</i> ,	
22	26 Cal. App. 4th 1225 (1994)	6
23	<i>Ruiz v. Gap Inc.</i> ,	
24	540 F. Supp. 2d 1121 (N.D. Cal. 2008), <i>aff’d</i> , 380 F. App’x 689 (9th Cir. 2010)	9
25	<i>SCC Acquisitions, Inc. v. Sup. Ct.</i> ,	
26	243 Cal. App. 4th 741 (2015)	10
27	<i>Schreiber Distrib. Co. v. Serv-Well Furniture Co.</i> ,	
28	806 F.2d 1393 (9th Cir. 1986)	2
	<i>Siva v. Gen. Tire & Rubber Co.</i> ,	
	146 Cal App. 3d 152 (1983)	18
	<i>In re Sony Gaming Networks</i> ,	
	903 F. Supp. 2d at 970	16
	<i>In re Sony Gaming Networks and Customer Data Security Breach Litigation</i> ,	
	996 F. Supp. 2d 942 (S.D. Cal. 2014).....	11

1	<i>Soule v. Gen. Motors Corp.</i> ,	
2	8 Cal. 4th 548 (1994)	5
3	<i>Tahoe Sierra Pres. Council, Inc. v. Tahoe Reg'l Planning Agency</i> ,	
4	34 F.3d 753 (9th Cir. 1994)	3
5	<i>Terpin v. AT&T Mobility, LLC</i> ,	
6	399 F. Supp. 3d 1035 (C.D. Cal. 2019) (Otis, J.)	7
7	<i>Therapeutic Res. Faculty v. NBTY, Inc.</i> ,	
8	488 F. Supp. 2d 991 (E.D. Cal. 2007).....	16
9	<i>Ticketmaster L.L.C. v. Prestige Entm't W., Inc.</i> ,	
10	315 F. Supp. 3d 1147 (C.D. Cal. 2018)	16
11	<i>Tyan, Inc. v. Garcia</i> ,	
12	2017 WL 1658811 (C.D. Cal. May 2, 2017)	16
13	<i>Vasquez v. Sup. Ct.</i> ,	
14	4 Cal. 3d 814, 94 Cal. Rptr. 796, 484 P.2d 964 (1971)	15
15	<i>Williams v. Sup. Ct.</i> ,	
16	3 Cal. 5th 531, 220 Cal. Rptr. 3d 472, 398 P.3d 69 (2017)	10
17	<i>In re Yahoo! Inc. Customer Data Security Breach Litig.</i> ,	
18	313 F. Supp. 3d 1113 (N.D. Cal. 2018)	11, 13, 14, 19
19	<i>Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC</i> ,	
20	774 F.3d 1065 (6th Cir. 2014)	17
21	Statutes	
22	18 U.S.C. § 1030.....	16
23	Federal Rules	
24	Fed. R. Civ. P. 8.....	1
25	Fed. R. Civ. P. 12(b)(6).....	1, 2
26	Fed. R. Civ. P. 15.....	2
27	Other Authorities	
28	Brian Rexroad, “Secure Your Number to Reduce SIM Swap Scams,” AT&T’s Cyber Aware (Sep. 2017), https://about.att.com/pages/cyberaware/ni/blog/sim_swap	18
	Cal Const., Art. 1, § I.....	10

1	Nathaniel Popper, <i>Hackers Hit Twitter C.E.O. Jack Dorsey in a ‘SIM Swap.’ You’re</i>	
2	<i>at Risk, Too.</i> , N.Y. TIMES (Sept. 5, 2019),	
3	https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-	
4	hack.html	15
5	Rest.2d Torts § 449	6
6	<i>Why Twitter Blames AT&T For The Hack Of Its CEO Jack Dorsey Account, Sending</i>	
7	<i>Shocking Racist Tweets</i> , FORBES (Aug. 31, 2019),	
8	https://www.forbes.com/sites/jeanbaptiste/2019/08/31/why-twitter-blames-att-	
9	for-ceo-jack-dorsey-account-hack-sending-shocking-racist-	
10	tweets/#5227d7dd2e30	15
11	Witkin & Epstein, Cal. Criminal Law § 130	7

1 I. INTRODUCTION

2 A team of criminals working for and with AT&T executed an unauthorized and illegal SIM
 3 swap of Robert Ross' phone, and then used their newfound access to reset the passwords to Mr.
 4 Ross' digital, financial accounts and ultimately steal over \$1 million from him. Unable to deny its
 5 involvement in these criminal acts, AT&T marshals a host of red herring, whataboutism inquiries
 6 to make it appear as though the theft of Mr. Ross' funds was utterly unforeseeable and unrelated
 7 to the SIM swap. But AT&T knows, and the Complaint clearly states, exactly *how* the theft
 8 occurred and *who* was involved in carrying out this brazen heist. The Court should therefore reject
 9 AT&T's stratagem as it seeks to obfuscate what the Complaint makes clear: AT&T knew, or should
 10 have known, that its portable SIM cards were an attack vector that was actively being exploited
 11 *before* the events at issue here, and AT&T failed to take adequate steps to remedy the situation.

12 At its core, the pending motion to dismiss Mr. Ross' Complaint rests on a fundamental
 13 distortion of the pleading standards under Rules 8 and 12(b)(6) of the Federal Rules of Civil
 14 Procedure. AT&T not only fails to accept Mr. Ross' well-pled factual allegations, but it also seeks
 15 to impose on him a "heightened fact pleading of specifics" which is contrary to the plausibility
 16 standard. *See Bell Atl. v. Twombly*, 550 U.S. 544, 570 (2007) ("we do not require heightened fact
 17 pleading of specifics, but only enough facts to state a claim to relief that is plausible on its face").
 18 To the extent AT&T has true inquiries about what happened, the parties should proceed to
 19 discovery.

20 In face of detailed allegations relating to how AT&T's conduct in Mr. Ross' SIM swap
 21 resulted in Mr. Ross' loss of over \$1 million, substantially all of which Mr. Ross held in US dollars
 22 (rather than cryptocurrency which AT&T implied), AT&T improperly insists upon a level of detail
 23 relating to proximate cause that is contrary to anything required at the pleading stage.

24 Equally improper, AT&T disregards its obligations to accept as true the facts alleged in the
 25 complaint and the reasonable inferences therefrom, and instead engages in a highly selective
 26 reading of the allegations in the complaint, including distorting quotes to change their meaning.

27 AT&T's motion to dismiss should be denied.

1 II. ARGUMENT

2 A. Standard of Review

3 A motion to dismiss under Rule 12(b)(6) challenges the legal sufficiency of the claims stated
 4 in the complaint. *See* Fed. R. Civ. P. 12(b)(6). To survive a motion to dismiss, the plaintiff's
 5 complaint "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that
 6 is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S.
 7 at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the
 8 court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*
 9 A complaint that offers mere "labels and conclusions" or "a formulaic recitation of the elements
 10 of a cause of action will not do." *Id.* In deciding a Rule 12(b)(6) motion, the Court must accept
 11 all allegations of material fact as true, construe the allegations in the light most favorable to the
 12 nonmoving party and draw all reasonable inferences in favor of the same. *Mangiaracina v.*
 13 *Penzone*, 849 F.3d 1191, 1198 (9th Cir. 2017); *Flores v. Adir Int'l, LLC*, 685 F. App'x 533, 534
 14 (9th Cir. 2017).

15 The court should freely grant a plaintiff leave to amend a deficient claim "when justice so
 16 requires." Fed. R. Civ. P. 15(a)(2). Where a motion to dismiss is granted, "leave to amend should
 17 be granted 'unless the court determines that the allegation of other facts consistent with the
 18 challenged pleading could not possibly cure the deficiency.'" *DeSoto v. Yellow Freight Sys., Inc.*,
 19 957 F.2d 655, 658 (9th Cir. 1992) (quoting *Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806
 20 F.2d 1393, 1401 (9th Cir. 1986)).

21 B. Mr. Ross Adequately Alleged Proximate Cause.

22 1. Mr. Ross Adequately Alleged How AT&T's Swapping of His SIM Card to a 23 Different Phone Led to the Loss of \$1 Million.

24 AT&T wrongfully characterizes Mr. Ross' detailed claims against it as "bare conclusions"
 25 and asserts that his allegations "lack[] *any explanation* of the sequence of events leading to his
 26 claimed loss." Mot. at 4–5 (emphasis added). It further claims "[a]t most, a SIM swap transfers
 27 control of a phone number." *Id.* at 5. This is incorrect, and to make that assertion, AT&T ignores
 28 entire pages of the Complaint detailing how a SIM swap is much more than a mere transfer of a

1 phone number. *See* Compl. ¶¶ 20–27, 37–40. Mr. Ross alleged in detail how the SIM swaps
 2 allowed hackers to access his digital accounts, and how the SIM swaps caused more than \$1
 3 million to be stolen from him.

4 Generally, causation—particularly proximate cause and the underlying foreseeability
 5 inquiry—is a question of fact for the jury. *Herrera v. Cnty. of Los Angeles*, 2013 WL 12121879,
 6 at *7 (C.D. Cal. Aug. 2, 2013); *Tahoe Sierra Pres. Council, Inc. v. Tahoe Reg’l Planning Agency*,
 7 34 F.3d 753, 756 (9th Cir. 1994) (noting in the context of a § 1983 claim that “a question of
 8 causation is preeminently a question of fact, to be decided after trial”); *Lies v. Farrell Lines, Inc.*,
 9 641 F.2d 765, 770 (9th Cir. 1981). Here, Mr. Ross has provided enough facts to adequately plead
 10 that AT&T’s conduct—acts and/or omissions—were the proximate cause of his loss of over \$1
 11 million.

12 In the Complaint, Mr. Ross explained that SIM swapping transfers control over a phone
 13 number, which includes not only texting and phone capabilities, but password reset capabilities.
 14 Compl. ¶¶ 20–27. AT&T’s claim that a SIM swap by itself “does not provide knowledge of or
 15 access to a cryptocurrency or another account”, Mot. at 5, is simply wrong. When an unauthorized
 16 SIM swap occurs, this effectively moves the victim’s phone service, and incoming data, texts, and
 17 calls to the phone controlled by the hacker. Compl. ¶¶ 23–25. This allows the hacker to exploit
 18 the two-factor authentication process, and either access the victim’s accounts without a password,
 19 or reset the password by having a reset code sent to the hacked phone via text messaging. *Id.* ¶
 20 24. AT&T cannot feign ignorance regarding these capabilities, including the foreseeable theft, that
 21 SIM swapping provides hackers, as the company itself has admitted that “SIM swapping . . .
 22 [provides] control over victims’ phone numbers” and that phones are “mini-computers” that
 23 contain “so much personal data”, “[our] life” and “everything.” *Id.* ¶¶ 81, 86. AT&T has also
 24 admitted that “most people do have something valuable [in their email accounts], which is access
 25 to all their other accounts, which you can get with a password reset.” *Id.* ¶ 85. In claiming that a
 26 SIM swap transfers *only* a phone number, AT&T illogically refuses to acknowledge that a SIM
 27 swap effectively transfers the key to the victim’s digital life—email, online banking, social media,
 28 etc.

1 By arguing that Mr. Ross did not provide any explanation of how the SIM swap lead to Mr.
 2 Ross' accounts being hacked, AT&T ignores the well-pled allegations in Mr. Ross' Complaint
 3 explaining how gaining control over a phone number is essentially gaining control over many
 4 digital accounts through two-factor authentication. Further, AT&T egregiously misquotes the
 5 Complaint and incorrectly claims that Mr. Ross said that hackers would also have needed to "steal[]
 6 [his] password" in order to gain control over his accounts. Mot. at 5. Instead, as alleged in the
 7 Complaint, a 2017 report by the U.S. Fair Trade Commission stated in relevant part:

8 Having a mobile phone account hijacked can waste hours of a victim's time and cause
 9 them to miss important calls and messages. *However, this crime is particularly*
 10 *problematic due to the growing use of text messages to mobile phones as part of*
 11 *authentication schemes for financial services and other accounts.* The security of two-
 12 factor authentication schemes that use phones as one of the factors relies on the
 13 assumption that *someone who steals your password has not also stolen your phone*
number. Thus, mobile carriers and third-party retailers need to be vigilant in their
 authentication practices to avoid putting their customers at risk of major financial loss
 and having email, social network, and other accounts compromised.

14 Compl. ¶ 77 (emphasis added).

15 At bottom, AT&T knew or should have known that a stolen phone can be as effective as a
 16 stolen password. It is simply not believable that AT&T is ignorant of these basic facts. If AT&T
 17 argues otherwise, following discovery, it is for a jury to determine.

18 Furthermore, contrary to another misquote by AT&T, Mr. Ross never pled that the SIM swap
 19 was "one of the factors" that hackers needed to gain control over his digital accounts. Mot. at 5.
 20 Instead, Mr. Ross alleged that through the SIM swap alone, hackers utilized two-factor
 21 authentication and gained control of additional accounts, such as his email, to access his accounts
 22 (by changing his password on those accounts). Compl. ¶¶ 28–40.

23 AT&T incorrectly argues that "[t]o gain access to cryptocurrency, one would need to also
 24 have account information—where the funds were located, who controlled the accounts in which
 25 they were held, and how to circumvent security to access those funds." Mot. at 5. As discussed
 26 *supra*, however, Mr. Ross adequately pled how hackers could use their control of his phone
 27 number, to find those funds—by accessing digital accounts (such as email). Specifically, Mr. Ross
 28 pled how hackers utilized his mobile phone number to take control over his most sensitive online

accounts, including his Authy and Google accounts.¹ Compl. ¶¶ 28–40. The hackers then used that access to take over his cryptocurrency accounts. *Id.*

In any event, under *Twombly*, this Court does not need specifics on how exactly hackers accessed Mr. Ross’ financial accounts. *Twombly* requires “only enough facts to state a claim to relief that is plausible on its face.” Further, as noted by California courts, proximate cause is a factual issue. *Herrera*, 2013 WL 12121879, at *7. Mr. Ross has alleged enough facts to state a plausible claim for relief, and any dispute about what happened is factual in nature and not appropriate to be dismissed at this stage.

2. Mr. Ross’ Allegations Do Not Rely on Unforeseeable Criminal Acts.

AT&T incorrectly argues that all of Mr. Ross’ claims for relief must fail for lack of causation because the harm was caused by the “independent intervening acts of others.” Mot. at 4, *quoting* *Martinez v. Pac. Bell*, 225 Cal. App. 3d 1557, 1565 (2003). This challenge must fail because AT&T improperly states California law, which clearly holds that foreseeable intervening events do *not* absolve a defendant of tort liability.²

As the California Supreme Court has definitively stated, “the defense of ‘superseding cause[]’ . . . absolves [the original] tortfeasor, even though his conduct was a substantial contributing factor, when an independent event [subsequently] intervenes in the chain of causation, producing harm of a kind and degree so far beyond the risk the original tortfeasor should have foreseen that the law deems it unfair to hold him responsible.” *Soule v. Gen. Motors Corp.*, 8 Cal. 4th 548, 573, n.9 (1994). “To determine whether an independent intervening act was reasonably foreseeable, [courts] look to the act and the nature of the harm suffered. To qualify as a superseding

¹ Authy is a mobile application that provides a “time-based one time password” that changes every 30 seconds. This password can be used to log into Mr. Ross’ cryptocurrency accounts. Hackers took control of Mr. Ross’ Authy to gain access to his cryptocurrency accounts. Compl. ¶¶ 37–40.

² Even assuming arguendo AT&T is right regarding Mr. Ross’ tort claims, it obviously cannot be true that Mr. Ross lacks proximate cause for *all* his claims. *See* Mot. at 1 (“AT&T moves to dismiss all claims...[a]s to all claims, Mr. Ross has failed to plausibly allege proximate cause) (emphasis added). Indeed, AT&T does not dispute that it violated the Federal Communications Act (“FCA” or “the Act”) and that it is liable to Mr. Ross for damages available under the Act. Moreover, proximate cause is a factor in torts involving liability for negligence, but it does not apply to, and has nothing to do with, claims for violation of a federal statute.

1 cause to relieve the defendant from liability for the plaintiff's injuries, both the intervening act and
 2 the results of that act must not be foreseeable. Significantly, 'what is required to be foreseeable is
 3 the general character of the event of harm . . . not its precise nature or manner of occurrence.'" *Chanda v. Fed. Home Loans Corp.*, 215 Cal. App. 4th 746, 701 (2013), *quoting Bigbee v. Pac. Tel.*
 4 *& Tel. Co.*, 34 Cal. 3d 49, 57–58 (1983) (emphasis added; additional internal citations omitted).

6 The California Supreme Court has further held that "[i]t is of no consequence that the injury
 7 to plaintiffs was brought about by the criminal acts of a third person. If the likelihood that a third
 8 person may act in a particular manner is the hazard or one of the hazards which makes the actor
 9 negligent, such an act whether innocent, negligent, intentionally tortious, or criminal does not
 10 prevent the actor from being liable for the harm caused thereby." *Isaacs v. Huntington Mem'l*
 11 *Hosp.*, 38 Cal. 3d 112, 131 (1985), *quoting* Rest.2d Torts § 449. Indeed, a defendant has a legal
 12 duty to protect against foreseeable criminal acts. *Campodonico v. State Auto Parks, Inc.*, 10 Cal.
 13 App. 3d 803, 807 (1970) ("Yet it is not the law that one has no duty to protect against foreseeable
 14 criminal acts."). California law also clearly holds that "[w]hether an intervening force is
 15 superseding or not generally presents a question of fact but becomes a matter of law where only
 16 one reasonable conclusion may be reached." *Chanda, supra*; *see also Rosh v. Cave Imaging Sys.,*
 17 *Inc.*, 26 Cal. App. 4th 1225, 1236 (1994) (question of whether individual's numerous unauthorized
 18 entries onto premises demonstrated defendant's lax security and foreseeability of harm to plaintiff
 19 factual question for jury). It is thus improper for AT&T to seek dismissal of Mr. Ross' claims on
 20 this ground because the foreseeability of the conduct is a factual issue that cannot be determined
 21 on a motion to dismiss. *See Isaacs*, 38 Cal. 3d at 135 (jury's determination of foreseeability can
 22 be based on "whether the occurrence of prior similar incidents placed the defendant on notice that
 23 its security measures were not adequate to prevent harm to persons who use the defendant's
 24 [services].").³

25 ³ AT&T ignores the significance of the word "independent" in citing to dicta in *O'Keefe v.*
 26 *Inca Floats, Inc.*, 1997 WL 703784, at *4 (N.D. Cal. Oct. 31, 1997), that "independent illegal acts
 27 of third parties" are "deemed unforeseeable and therefore, the sole proximate cause of the injury
 28 which excludes negligence of another as a cause of the injury." An "independent" act is a term of
 art under California law meaning an act "so disconnected and unforeseeable as to be a superseding

Moreover, in a substantially similar case, the Central District of California recently rejected AT&T's argument that it should not be held liable for the criminal acts of a third party. *See Terpin v. AT&T Mobility, LLC*, 399 F. Supp. 3d 1035, 1044 (C.D. Cal. 2019) (Otis, J.). In *Terpin*, the plaintiff alleged that he notified AT&T in June 2017 that he was the victim of a SIM swap and that AT&T placed his account on a higher security level with special protection. *Id.* Despite this actual notice that the plaintiff's account was at risk, however, the plaintiff's account was again the victim of a SIM swap in January 2018, which was facilitated by the criminals working for AT&T. *Id.* The court therefore concluded that the plaintiff had "sufficiently alleged that the criminal act was reasonably foreseeable such that the claim should not be dismissed on this basis." *Id.* This Court should reach the same conclusion here. Indeed, the facts in *Terpin* provide evidence that AT&T understands the foreseeable criminal conduct prompted by a SIM swap.

AT&T was specifically put on notice there was abnormal and troubling activity occurring on Mr. Ross' account and yet went ahead and conducted a SIM swap. An AT&T employee informed Mr. Ross that the SIM swap was executed despite it being a "direct violation" of AT&T policies. *Id.* ¶ 34. Further, AT&T should have known this SIM swap was likely, as the hacker involved in Mr. Ross' SIM swap had requested over *eleven different phone numbers* be moved onto his phone in the three weeks *before* Mr. Ross's swap. *Id.* ¶ 109. In fact, that hacker sometimes moved three different AT&T numbers onto his phone in a single day. *Id.* Despite the fact that the phone to which Mr. Ross' phone number was swapped had extremely abnormal and troubling activity, Mr. Ross' SIM card was swapped. This violation of AT&T policy resulted in the loss of \$1 million and the compromise of Mr. Ross' extremely personal data, including his and his daughter's passports, drivers' licenses, birth certificates, and his sensitive tax data. *Id.* ¶¶ 43–45.

cause, i.e., in such a case the defendant's act will be a remote and not the proximate cause." *People v. Schmies*, 44 Cal. App. 4th 38, 49 (1996) (emphasis added), *quoting* Witkin & Epstein, Cal. Criminal Law § 130, p. 148. Plaintiffs' citation in *Jesse v. Malcmacher*, 2016 WL 9450683 (C.D. Cal. Apr. 5, 2016), to dicta in *O'Keefe*, *supra*, that "illegal acts of third parties are unforeseeable as a matter of law" unfortunately omits the key word "independent" signifying that the intervening act itself must be unforeseeable. This qualifying interpretation of the word "independent" is the only reasoned way to reconcile *O'Keefe* with the settled law cited in these papers.

AT&T's should have had adequate security measures in place to guard against the highly foreseeable and likely act that hackers would actively seek to obtain the personal information of AT&T customers. The prevalence of hacking is not only highly publicized (and thus generally foreseeable) but was specifically an issue in this case because AT&T is statutorily required to guard against hackers in order to protect customers' personal information. *Id.* ¶¶ 89–94. Additionally, Mr. Ross alleged that AT&T knew or should have known about the risk of SIM swap crimes, as it has been a growing problem that the FTC has warned mobile carriers about well before his SIM swap. *Id.* ¶¶ 76–80. In fact, AT&T was warned by the FTC that it should “adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions.” *Id.* ¶ 77. AT&T itself admitted that its customers with “valuable accounts that are accessible online” are likely targets of SIM swaps. *Id.* ¶ 78. Further, AT&T's Vice President of Security noted that hackers were “conducting SIM swap[] attacks to seize control over victims' phone numbers.” *Id.* ¶ 86. AT&T has also advised that “[your] phone is [your] life” and it is necessary to think about “what would a hacker want to do, where would a hacker go to get [] data, what are some of the points on [] the network that are most vulnerable, or where is the flow that is potentially going to be a leakage.” *Id.* ¶¶ 81–82.

Given AT&T's *own admonition* to customers about the risks of SIM swaps, its claims that Mr. Ross' SIM swap was caused by unforeseeable events ring hollow. The Court should reject AT&T's arguments regarding proximate causation.

C. Mr. Ross' Right to Privacy Claim Under the California Constitution (Count III) Should Not Be Dismissed Because He Adequately Pled that Actions By AT&T's Employees Constitute an Egregious Breach of Social Norms.

AT&T misconstrues the facts and incorrectly asserts that Mr. Ross claimed that AT&T negligently invaded his privacy. Mr. Ross pled that AT&T, through its employees, *intentionally* invaded his privacy. Indeed, Mr. Ross pled (and law enforcement has confirmed) that AT&T employees conducted a COAM-originated SIM swap (which violates company policy) to a phone

1 that had *eleven different* numbers swapped onto it in the three weeks before that swap.⁴ *Id.* ¶ 41.
 2 This was not mere negligence on the part of the AT&T employees; it was intentional. *Id.* ¶¶ 33–
 3 34, 56, 106, 109.

4 The two cases AT&T cites in opposition are inapposite here. In *Ruiz v. Gap Inc.*, the court
 5 found that an “increased risk of identity theft” did not create a violation of California Constitutional
 6 Right to Privacy claim. 540 F. Supp. 2d 1121, 1124 (N.D. Cal. 2008), *aff’d*, 380 F. App’x 689 (9th
 7 Cir. 2010). There, the plaintiff claimed the defendant negligently permitted laptop computers
 8 containing unencrypted personal information of job applicants to be stolen. *Id.* Similarly, *In re*
 9 *iPhone Litigation*, the court denied the plaintiffs right to privacy claim because the plaintiff alleged
 10 that the invasion of privacy was caused by Apple’s *negligence*. 844 F. Supp. 2d 1040, 1064 (N.D.
 11 Cal. 2012)

12 Here, unlike those two cases, Mr. Ross does not claim AT&T invaded his privacy merely by
 13 its negligence. He claims that the invasion of privacy claim stems from purposeful and/or
 14 extremely reckless actions by AT&T, through its employees. Compl. ¶¶ 144–53.

15 **D. Mr. Ross Specifically Alleged What Information AT&T Disclosed.**

16 AT&T also incorrectly contends that Mr. Ross did not allege what private information AT&T
 17 disclosed.

18 Mr. Ross pled that AT&T, through his employees, accessed his Customer Proprietary
 19 Network Information (“CPNI”) in order to effectuate the unauthorized SIM swap. *Id.* ¶¶ 53, 56,
 20 119. This private information is statutorily protected under the FCA. *Id.* ¶¶ 89–94. He specifically
 21 pled the compromise of this sensitive data, and his pleading was not “generic” and “non-specific”,
 22 as AT&T claims. Mot. at 11. The exposure and dissemination of this data is sufficient to establish
 23 a claim for invasion of privacy. *See* Cal Const., Art. 1, § I (“All people are by nature free and
 24

25 _____
 26 ⁴ Customer owned and maintained (“COAM”) equipment is a mobile phone that is not
 27 provided by AT&T and would generally be of unknown origin to AT&T (for example, a used
 28 mobile phone purchased on the internet). Compl. ¶ 34. It is against AT&T internal policies for an
 AT&T representative to execute a COAM-originated SIM swap request from anyone calling in
 to an AT&T call center. *Id.*

independent and have inalienable rights. Among these are . . . pursuing and obtaining safety, happiness and privacy.”). Courts construing this constitutional guarantee have held that “[t]he right of privacy protects against the unwarranted, compelled disclosure of private or personal information” and protects from public disclosure “the details of one’s private life.” *SCC Acquisitions, Inc. v. Sup. Ct.*, 243 Cal. App. 4th 741, 754 (2015).

Though alleging that AT&T exposed his CPNI is enough to adequately allege a breach of privacy claim, Mr. Ross also pled that AT&T permitted others to access Mr. Ross’ account and the confidential information it contained by conducting the SIM swap against company policies. Compl. ¶¶ 33–35. Mr. Ross further pled that, due to AT&T’s illegal and unauthorized SIM swap, his and his family’s highly sensitive data, including color copies of their passports, their social security numbers, driver’s licenses, birth certificates, and financial information, including his tax returns were accessed illegal and are now permanently compromised, which pose innumerable and critical identity fraud risks to Mr. Ross and his minor daughter for the rest of their lives. *Id.* ¶ 45. This type of information is protected by the California Constitution. *See, e.g., Williams v. Sup. Ct.*, 3 Cal. 5th 531, 554, 220 Cal. Rptr. 3d 472, 398 P.3d 69 (2017) (noting that medical history, financial data, and home contact information is generally considered private); *Henson v. Turn, Inc.*, 2018 WL 6605624, at *4 (N.D. Cal. 2018) (noting the confidentiality of individually identifiable information, such as social security numbers); *Cabral v. Supple, LLC*, 2012 WL 12895825, at *3 (C.D. Cal. Oct. 3, 2012) (noting that there is heightened expectation of privacy warranting additional protection for financial information).

These purposeful and/or reckless actions by AT&T employees to disseminate Mr. Ross’ private information, including his CPNI, constitute a violation of Mr. Ross’ constitutional right to privacy.

E. Mr. Ross’ Claims for Negligence and Negligent Supervision and Entrustment (Counts IV and V) Should Not Be Dismissed, Given the Existence of a Special Relationship.

AT&T’s conclusion that the special relationship exception to the economic loss rule is inapplicable here is flatly contradicted by numerous facts. The special exception can apply to

parties with contracts for services (as opposed to goods), thus rendering the economic loss rule inapplicable, as made clear by a veritable legion of legal precedent.⁵ In this case, there is no doubt that AT&T’s negligence involved its “services.” AT&T provides telecommunications or wireless “services” (often provided in conjunction with the sale of a mobile telephone). Compl. Ex. C (“Our Privacy Policy applies to your use of all products, **services**, and websites offered by AT&T . . .”) (emphasis added). *See also In re Yahoo! Inc. Customer Data Security Breach Litig.*, 313 F. Supp. 3d 1113, 1132 (N.D. Cal. 2018), (finding that plaintiffs had adequately alleged that Yahoo provided a “service” to Plaintiffs by providing email-service through accounts on a web-based platform).

Second, Mr. Ross has adequately pled enough facts to plausibly meet the *J’Aire* factors to establish a special relationship, which is all that is necessary at this stage. To determine whether a special relationship exists, courts consider six factors: “(1) the extent to which the transaction was intended to affect Mr. Ross, (2) the foreseeability of harm to the plaintiff, (3) the degree of

⁵ *E.g., N. Am. Chem. Co. v. Sup. Ct.*, 59 Cal. App. 4th 764, 777 (1997) (holding the economic loss rule does not apply to allegedly negligent performance of contract for packing and shipping services); *CoreLogic, Inc. v. Zurich Am. Ins. Co.*, 2016 WL 4698902, at *5 (N.D. Cal. Sept. 8, 2016) (economic loss rule did not preclude claims for economic losses for negligent performance of professional services); *Cytokinetics, Inc. v. Pharm-Olam Int’l, Ltd.*, 2015 WL 1056324, at *6 (N.D. Cal. Mar. 10, 2015) (“In some circumstances negligent performance of a contract may be actionable as a tort, and California courts have held that the economic loss rule will not apply where the contract in question involves defective services rather than defective products.”); *Ladore v. Sony Computer Entm’t Am., LLC*, 75 F. Supp. 3d 1065, 1075–76 (N.D. Cal. 2014) (“*Ladore* correctly notes that in *North American Chemical*, the Court of Appeal concluded that the Plaintiff’s negligence cause of action was **not** barred by the economic loss rule at the pleading stage. But *Ladore* fails to recognize that this was because *North American Chemical* concluded that the economic loss rule does not necessarily apply in cases arising out of ‘a contract for the performance of services rather than the sale of goods.’”) (emphasis in original); *City & Cnty. of San Francisco v. Cambridge Integrated Servs. Grp, Inc.*, 2007 WL 1970092, at *2 (N.D. Cal. July 2, 2007) (finding California courts “distinguish[] cases involving defective products, for which the economic loss rule applies, and those involving defective services, for which the economic loss rule does not apply”); *Moreno v. Sanchez*, 106 Cal. App. 4th 1415, 1435 (2003) (“Under the common law the established rule is the negligent failure to exercise reasonable care and skill in undertaking to perform a service contract of this type is a tort, as well as a breach of contract.”). Furthermore, AT&T’s reliance on *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 969 (S.D. Cal. 2014) is misplaced. In that case, plaintiffs acknowledged that the Defendant did not owe them a legal duty to provide their service, whereas here, AT&T owes Mr. Ross a legal duty to protect his CPNI and other sensitive data.

1 certainty that the plaintiff suffered injury, (4) the closeness of the connection between the
 2 defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's
 3 conduct and (6) the policy of preventing future harm.” *J’Aire Corp. v. Gregory*, 24 Cal. 3d 799,
 4 804 (1979).⁶

5 In *Fields v. Wise Media, LLC*, the court denied defendants’ motion to dismiss after the
 6 plaintiffs “asserted sufficient facts to plausibly meet the second, third, fourth, fifth, and sixth *J’Aire*
 7 factors,” 2013 WL 5340490, at *3 (N.D. Cal. Sept. 24, 2013), holding that plaintiffs had pled an
 8 adequate negligence claim to survive a motion to dismiss.

9 Here, under the first factor, the contract between AT&T and Mr. Ross was intended to affect
 10 him; Mr. Ross chose AT&T as his wireless service provider, thereby disclosing his personal
 11 information (including CPNI), in exchange for, and only because of, AT&T’s promise and
 12 representations that it would adequately protect such information. As AT&T has noted, an
 13 individual’s phone is their “life” and contains extremely personal information on it. Compl. ¶¶
 14 81–82. In its privacy policy, AT&T promised to keep Mr. Ross’ “personal information safe” and
 15 use “other security safeguards to protect customer data.” *Id.*, Ex. B. The privacy policy between
 16 the two parties was intended to affect Mr. Ross. AT&T misreads the case law and incorrectly
 17 argues that the transaction must affect Mr. Ross in a “particular way as opposed to all potential
 18 consumers” for the special relationship exception to apply. Mot. at 16–17. Under, the *J’Aire* test,
 19 only if the party asserting negligence is a third-party to a contract does the analysis hinge on
 20 whether the transaction was supposed to affect the plaintiff in a “particular” way. *Ray v. BlueHippo*
 21 *Funding, LLC*, 2008 WL 1995113, at *6 (N.D. Cal. May 6, 2008) (“A critical foundational
 22 requirement for finding a special relationship is whether the **third-party transaction** was intended
 23 to affect the plaintiff in a particular way[.]”) (emphasis added); *Dubbs v. Glenmark Generics Ltd.*,
 24 2014 WL 1878906, at *6 (C.D. Cal. May 9, 2014) (noting that if “the manufacturer had **specific**

25
 26
 27 ⁶ Subsequent cases have held that whether a special relationship exists is determined
 28 primarily by the first four *J’Aire* factors. See *Ott v. Alfa-Laval Agri, Inc.*, 37 Cal.Rptr.2d 790, 798,
 31 Cal.App.4th 1439, 1450 (Cal.App. 5 Dist. 1995).

1 *knowledge* of a particular party, then that party could potentially go forward with a tort action”
 2 under the special relationship-exception) (emphasis added).

3 Further, California courts have found the first *J’Aire* factor exists in cases where the contract
 4 or transaction affected the plaintiff the same way as all other “potential consumers” to the
 5 transaction. *Yahoo II* (finding first factor exists even when a class of plaintiffs asserted it); *Corona*
 6 *v. Sony Pictures Entm’t, Inc.*, 2015 WL 3916744, at *1 (C.D. Cal. May 9, 2015) (finding that
 7 requiring plaintiffs to provide personal information to the defendant was a “transaction . . . intended
 8 to affect Plaintiffs”, even though the transaction affected *all* of defendant’s employees the same
 9 way); *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *5 (N.D. Cal. Sept. 14, 2016) (finding
 10 existence of the first *J’Aire* factor although the transaction at issue affected all employees the same
 11 way, not just the employees asserting the claim). *See also J’Aire Corp.*, 157 Cal. Rptr. at 410 (“The
 12 contract entered into between respondent and the county was for the renovation of the premises in
 13 which appellant maintained its business. The contract could not have been performed without
 14 impinging on that business. Thus, respondent’s performance was intended to, and did, directly
 15 affect appellant.”).

16 Under the second factor, the harm to Mr. Ross was foreseeable. As discussed *supra* in
 17 Section B, AT&T was aware or should have been aware of numerous unauthorized and illegal SIM
 18 swaps conducted by its representatives and the danger the attacks posed to its users’ data. In a
 19 similar case, *In re Yahoo!*, *supra* at 1132, the court found it was “plainly foreseeable that Plaintiffs
 20 would suffer injury if [Yahoo] did not adequately protect the [plaintiffs’ personal information].”

21 Under the third factor, the Mr. Ross adequately pled that he suffered injury because of
 22 AT&T’s negligence. He pled that he lost over \$1 million and that his private data, including his
 23 CPNI, driver’s licenses, birth certificate, passport, and financial data were compromised. Compl.
 24 ¶¶ 43–45. At bottom, Mr. Ross adequately pled that he suffered both financially and emotionally.
 25 *Id.* ¶ 44.

26 Under the fourth factor, the “closeness of the connection between the defendant’s conduct
 27 and the injury suffered”, Mr. Ross adequately pled that he suffered injury *because* of AT&T’s
 28 negligence and intentional conduct. As explained in Section B, *supra*, but for AT&T’s negligence

1 and purposeful actions, Mr. Ross would not have been robbed of \$1 million, and his personal data
 2 would not have been compromised. *See, e.g., N. Am. Chem. Co. v. Sup. Ct.*, 69 Cal. Rptr. 2d 466,
 3 479, (Cal. App. 2 Dist. 1997) (finding factor four of the *J'Aire* existed where “the injury resulted
 4 directly from [the defendants’] negligent acts”).

5 Under the fifth factor, moral blame should be assigned to AT&T. AT&T was, or should have
 6 been, aware that there was extremely abnormal and likely malicious activity on the phone to which
 7 Mr. Ross’ number was swapped, and it did nothing to stop the swaps or flag that number. Even a
 8 rudimentary flag that the phone (to which Mr. Ross service was to be swapped) had recently been
 9 involved in numerous SIM swaps could easily have been put in place by AT&T, which would
 10 have averted the nightmare to which AT&T has subjected Mr. Ross and his family. AT&T executed
 11 eleven different, malicious SIM swaps onto a phone controlled by the hackers it was working with
 12 *prior* to Mr. Ross’ SIM swap. AT&T did nothing to stop this activity. Indeed, Mr. Ross pled that
 13 AT&T told him his SIM card was swapped in direct violation of its policies. Compl. ¶¶ 33–35.
 14 As in *In re Yahoo!*, *supra*, at 1132, AT&T “knew their data security was inadequate” and that “they
 15 [did not] have the tools” to stop the compromise of user’s personal data. As with the court’s finding
 16 in *In re Yahoo*, the fifth factor is met here because “[d]efendants are morally culpable, given their
 17 repeated security breaches, wholly inadequate safeguards, and refusal to notify [p]laintiffs . . . of
 18 breaches or security vulnerabilities.” *Id.*

19 Finally, under the sixth factor, AT&T has not articulated a policy to prevent future harm to
 20 Mr. Ross. His data, including his CPNI, was breached, he had over \$1 million stolen from him,
 21 and AT&T has not attempted to make Mr. Ross whole. AT&T argues it has “strong incentives” to
 22 avoid fraudulent SIM swaps, Mot. at 18, and yet Mr. Ross was SIM swapped onto a phone with
 23 malicious activity, and AT&T has done nothing to prevent this from happening in the future.
 24 Indeed, AT&T has admitted to Mr. Ross that it violated its own policies by effecting the SIM swap,
 25 yet it has done nothing to materially change its policies or the execution of those policies.⁷

26 _____
 27 ⁷ The court should also take judicial notice of the fact that there have been numerous,
 28 unauthorized SIM swaps on AT&T phones, including a high profile attack against billionaire Jack
 Dorsey, which result in one or more of the victim’s digital accounts being hacked. *See* Nathaniel

Accordingly, Mr. Ross has pled facts to establish all six factors of the *J'Aire* special relationship exception, and the motion to dismiss his negligence and negligent supervision and entrustment claims should be denied.

F. Under the CLRA, Mr. Ross Adequately Pled Actual Reliance Based on His Reliance On AT&T's Privacy Policy.

Further, Mr. Ross adequately pled reliance on AT&T's material misrepresentations—specifically, its statements that it would not sell his personal information, protect his privacy, and keep his personal information safe. Compl. ¶ 4. California courts have found that if material misrepresentations were made to individuals . . . there is an inference of reliance. *Mass Mut. Life Ins. Co. v. Sup. Ct.*, 119 Cal. Rptr. 2d 190, 197, 97 Cal. App. 4th 1282, 1292–93 (Cal. App. 4 Dist. 2002); *Vasquez v. Sup. Ct.*, 4 Cal. 3d 814, 94 Cal. Rptr. 796, 484 P.2d 964 (1971). California courts also have found a CLRA violation when companies violate privacy policies. *See Doe I v. AOL LLC*, 719 F. Supp. 2d 1102, 1113 (N.D. Cal. 2010) (finding a valid CLRA claim against AOL for violating its privacy policy).

Here, Mr. Ross chose to purchase a phone and SIM card, and subscribe to AT&T service, based on AT&T's representations regarding its privacy practices and its Privacy Policy about how it would handle and protect his data. Compl. ¶¶ 99–123. This misrepresentations and omissions are material, and this court should infer that Mr. Ross relied on these statements from AT&T's 2006 Privacy Policy when he signed up for AT&T. To the extent the Court concludes Mr. Ross has not pled actual reliance and cannot rely on an inference of reliance, Mr. Ross respectfully requests that leave to amend should be granted to plead actual reliance. *See In re Sony Gaming*

Popper, *Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too.*, N.Y. TIMES (Sept. 5, 2019), <https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html>; Jeb Su, *Why Twitter Blames AT&T For The Hack Of Its CEO Jack Dorsey Account, Sending Shocking Racist Tweets*, FORBES (Aug. 31, 2019), <https://www.forbes.com/sites/jeanbaptiste/2019/08/31/why-twitter-blames-att-for-ceo-jack-dorsey-account-hack-sending-shocking-racist-tweets/#5227d7dd2e30>. The Court may, of course take judicial notice of matters of public record and publicly accessible websites whose accuracy and authenticity is not subject to dispute. *In re Facebook, Inc. Sec. Litig.*, 405 F.Supp.3d 809, 827 (N.D. Cal. 2019).

1 *Networks*, 903 F. Supp. 2d at 970 (granting plaintiffs leave to amend complaint to plead actual
2 reliance).

3 **G. Mr. Ross Adequately Pled Qualifying Loss Under the CFAA.**

4 Under the CFAA, loss is defined as “any reasonable cost to any victim, including the cost of
5 responding to an offense, conducting a damage assessment, and restoring the data, program,
6 system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or
7 other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11).
8 These nine types of loss are examples, not limitations on what qualifies as “loss” under the CFAA.
9 *Ticketmaster L.L.C. v. Prestige Entm’t W., Inc.*, 315 F. Supp. 3d 1147, 1173–74 (C.D. Cal. 2018);
10 *see, e.g., Tyan, Inc. v. Garcia*, 2017 WL 1658811, at *14 (C.D. Cal. May 2, 2017). To prevail on
11 a CFAA claim, a plaintiff must show “loss to 1 or more persons during any 1-year period . . .
12 aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(c)(4)(A)(i)(I).

13 AT&T’s claims that Mr. Ross did not adequately plead qualifying loss in the complaint and
14 that loss is primarily “the remedial costs of investigating a computer for damage, remedying
15 damage done, and costs incurred while the computer is inoperable,” Mot. at 21–22. These
16 arguments fail for two reasons.

17 First, all but one of the cases AT&T cites are out-of-circuit cases that define loss differently
18 than California courts do. To be sure, California courts are split on how they define loss, but better
19 reasoned cases have found that loss can be any of the types of damages listed under the statutory
20 language (and indeed, that the list is not exhaustive). *See, e.g., Tyan*, 2017 WL 1658811, at *14
21 (losses awarded under CFAA included various cost of repair to lost and damaged files, the fair
22 market value of targeted files, and ***company’s lost profits as a result of the hack***); *Therapeutic*
23 *Res. Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991, 995–97 (E.D. Cal. 2007) (finding loss where a
24 CFAA violation caused plaintiff to lose \$40,000 in profits); *In re: Lenovo Adware Litig.*, 2016 WL
25 6277245, at *6 (N.D. Cal. Oct. 27, 2016) (Allowing a CFAA claim to proceed when plaintiff
26 alleged that he suffered losses as a result of computer performance issues and suspected privacy
27 intrusions which interrupted service right before filing date for income taxes.). Other circuits agree
28

1 with California’s definition. *See, e.g., Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*,
 2 774 F.3d 1065, 1073–74 (6th Cir. 2014) (“If a plaintiff is able to establish a loss of at least \$5,000
 3 in value, whether that be composed solely of costs identified in the first clause, or solely costs
 4 identified in the second clause, or a combination of both, then he may recover under the statute.”).

5 Second, contrary to AT&T’s assertions, Mr. Ross pled “additional facts” to meet his pleading
 6 burden. Specifically, he pled that he lost over \$1 million due to the interruption of his service.
 7 Compl. ¶¶ 29–40. Further, Mr. Ross pled that he has spent over \$5,000 trying to investigate who
 8 accessed his device and damaged the information on it. *Id.* ¶ 202. Nothing more is required at this
 9 stage. Indeed, in *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 962 (N.D. Cal. 2014),
 10 the court found that the plaintiff satisfied its pleading requirement for the CFAA’s loss requirement
 11 by alleging that the plaintiff’s employees spent substantial time and energy “on their efforts to
 12 secure the restoration of *NovelPoster* and its data and information” to the condition they were in
 13 “prior to when defendants took control of *NovelPoster*,” and that these efforts included restoring
 14 the data and information to their prior condition, as well as responding to and conducting a damage
 15 assessment of defendants’ alleged CFAA violation. Here, Mr. Ross has pled his loss in more detail
 16 than the plaintiffs in *NovelPoster*. Moreover, in *NovelPoster* the court also noted that defendant’s
 17 argument required “a factual inquiry into the accuracy of [the plaintiff’s] claims that is not
 18 appropriate on a motion for judgment on the pleadings.” AT&T’s arguments also require factual
 19 inquiries that are not appropriate at this stage.

20 The motion to dismiss the CFAA claim should be denied. To the extent the Court concludes
 21 Mr. Ross has not pled loss under the CFAA, however, Mr. Ross respectfully requests that leave to
 22 amend should be granted to plead loss in more detail, specifically the costs associated with
 23 investigating his phone for damage, remedying that damage, and the costs incurred while his phone
 24 was inoperable.

25 **H. Punitive Damages Should Not be Stricken.**

26 AT&T claims that Mr. Ross’ punitive damages claim should be stricken because he did not
 27 allege that the employee conduct referenced in the Complaint was directed or ratified by AT&T’s
 28

1 officers, directors or managing agents. Mot. at 24. Because issues relating to ratification of
 2 employee conduct are quintessentially factual, however, they cannot be resolved on a motion to
 3 dismiss. *See Siva v. Gen. Tire & Rubber Co.*, 146 Cal App. 3d 152, 159 (1983) (“[r]atification is
 4 a fact question and may be proved by circumstantial evidence.”). In addition, the question of
 5 whether an individual is a managing agent or has been authorized by an employer is a “fact-
 6 intensive inquiry.” *Paterson v. Cal. Dept. of Gen. Servs.*, 2008 WL 4737118 at *4 (E.D. Cal. Oct.
 7 28, 2008). Given the factual nature of the inquiry, punitive damages may only be barred at the
 8 motion to dismiss stage where they are unavailable as a matter of law. *See, e.g., Rios v. City of*
 9 *Bakersfield*, 2011 WL 5554506, at *6 (E.D. Cal. Nov. 15, 2011) (dismissing punitive damages
 10 claim against municipality because such damages are precluded as a matter of law). That said,
 11 Ross has properly alleged a basis for punitive damages.

12 In great detail, Mr. Ross has alleged the history of the initial SIM swap fraud, including
 13 informing AT&T that he had been a victim of hacking to his mobile account and the promises made
 14 by AT&T employees to provide him with additional protection to prevent such fraud in the future.
 15 Compl. ¶¶ 29–35. AT&T was under both a statutory obligation and a duty imposed by the FCC in
 16 a 2015 Consent Decree to protect the personal information of its customers against fraud. *Id.* ¶¶
 17 89–94. AT&T was aware that its employees could bypass protections, and in certain instances,
 18 acted in concert with hackers to turn over its customers’ personal information. *Id.* Moreover,
 19 AT&T’s Vice President promised that AT&T knew that SIM swap thieves were constantly
 20 changing their tactics and that AT&T would continually enhance its safety measures in response.
 21 *Id.* ¶ 78, n.43 (citing Brian Rexroad, “Secure Your Number to Reduce SIM Swap Scams,” AT&T’s
 22 Cyber Aware (Sept. 2017), https://about.att.com/pages/cyberaware/ni/blog/sim_swap). AT&T
 23 consciously disregarded these obligations by failing to supervise its employees and permitting a
 24 system to exist where employees could readily bypass account protections. *Id.* ¶¶ 154–82.

25 Under these circumstances, Mr. Ross’ allegations sufficiently allege a basis for punitive
 26 damages beyond the allegedly “conclusory” allegations of the claims themselves. *See Exxon*
 27 *Mobil Oil Corp. v. S. Cal. Edison Co.*, 2013 WL 12166214 at *3 (C.D. Cal. May 1, 2013) (holding
 28 that complaint that “extensively alleges the history of past outages and litigations” sufficiently and

1 plausibly alleged punitive damages); *Khan v. 7-Eleven, Inc.*, 2015 WL 12743691, at *3 (C.D. Cal.
 2 Nov. 15, 2015) (finding that allegations of conduct of 7-Eleven employee taken in the light most
 3 favorable to plaintiff sufficiently alleged punitive damages under *Iqbal*).

4 Considering the allegations of the Complaint as a whole, Mr. Ross' allegations also support
 5 his contention that AT&T had the requisite mental state and acted with malice, fraud and
 6 oppression. Construing the allegations of the Complaint in the light most favorable to Plaintiff
 7 (which the Court is required to do), the allegations show that AT&T acted with fraud, malice and
 8 oppression in violating its statutory duties under Section 222(a) of the FCA and in its actions
 9 specific to Mr. Ross. Further, under *In re Yahoo!*, *supra*, the Court should not dismiss Plaintiff's
 10 punitive damage requests for its claims for negligence and negligent supervision and hiring.

11 As the Court in *In re Yahoo!* properly observed, "even where the claim formally sounds in
 12 negligence, if the plaintiff can make a showing that defendant's conduct goes beyond gross
 13 negligence and demonstrates a knowing and reckless disregard, punitive damages may be
 14 available.'" *In re Yahoo!*, *supra* at 1149, *quoting Simplicity Int'l v. Genlabs Corp.*, 2010 WL
 15 11515296, at *2 (C.D. Cal. Apr. 21, 2010). Like in *In re Yahoo!*, in this litigation, Mr. Ross has
 16 "alleged numerous fraudulent, malicious, and oppressive acts on the part of Defendant[]." The
 17 Court should therefore not dismiss the punitive damages requests for Mr. Ross' claims based in
 18 negligence.

19 **III. CONCLUSION**

20 For the foregoing reasons, the Court should deny AT&T's Motion to Dismiss.
 21
 22
 23
 24
 25
 26
 27
 28

1 Dated: January 8, 2020

Respectfully submitted,

2 

3 Thomas D. Warren (SBN No.160921)

4 twarren@piercebainbridge.com

Andrew Calderón (SBN No. 316673)

5 acalderon@piercebainbridge.com

6 **PIERCE BAINBRIDGE BECK PRICE
& HECHT LLP**

7 355 S. Grand Avenue, 44th Floor,

8 Los Angeles, CA 90071

Telephone: (213) 262-9333

9 Facsimile: (213) 279-2008

10 Dwayne D. Sam (admitted *pro hac vice*)

11 dsam@piercebainbridge.com

12 **PIERCE BAINBRIDGE BECK PRICE
& HECHT LLP**

13 600 Pennsylvania Avenue NW

14 South Tower, Suite 700

15 Washington, DC 20004

16 Telephone: (202) 843-8342

17 Facsimile: (646) 968-4125